

Contents

Part I Synopsis

1	Introduction	3
1.1	Motivation and Problem Statement	3
1.2	Aims and Objectives	5
1.3	Structure of the Work	7
1.4	Underlying Publications and Contributions of the Author	11
2	Theoretical Background and Related Work	17
2.1	Peace and Conflict Studies	17
2.2	Technology Assessment and Design	23
2.3	Research Gap	28
3	Research Design	31
3.1	Conceptual Background	31
3.2	Research Approach	34
3.3	Research Context	36
3.4	Methods	37
4	Results	43
4.1	Monitoring Perspective: Military and Civilian Applications	43
4.2	Governance Perspective: Weapons and non-Weapon Systems	48
4.3	Design Perspective: ICT Research and Development of Concern	52
4.4	Summary of Results	56

5	Discussion	59
5.1	Monitoring of Dual-use ICTs	59
5.2	Governance of Dual-use ICTs	61
5.3	Design of Dual-use ICTs	63
5.4	Towards Dual-Use Assessment of ICTs	65
5.5	Limitations and Future Work	67
6	Conclusion	69
7	List of the Author's Publications	71

Part II Publications

8	Measuring Spillover Effects from Defense to Civilian Sectors: A Quantitative Approach Using LinkedIn	79
8.1	Introduction	79
8.2	State of Research	81
8.3	Analyzing the LinkedIn Profile Data	84
8.4	Empirical Results	86
8.5	Comparison of the Approaches	89
8.6	Conclusion	90
9	Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion between Civilian and Defense R&D	93
9.1	Introduction	93
9.2	Related Work and Theoretical Background	95
9.3	Research Design	99
9.4	Analysis	102
9.5	Discussion	106
9.6	Conclusion	109
10	Meaningful Human Control of LAWS: The CCW-Debate and its Implications for Value-Sensitive Design	111
10.1	Introduction	111
10.2	Related Work	113
10.3	Theoretical Background	115
10.4	Research Design	116
10.5	Results	119
10.6	Discussion and Conclusion	129

11	U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance	133
11.1	Introduction	133
11.2	Related Work	135
11.3	Method	139
11.4	Results	142
11.5	Discussion	152
11.6	Conclusion	156
12	Values and Value Conflicts in the Context of OSINT Technologies for Cybersecurity Incident Response	157
12.1	Introduction	157
12.2	Background and Related Work	159
12.3	Methods	163
12.4	Results	168
12.5	Discussion and Implications	182
12.6	Conclusion	190
13	Computer Emergency Response Teams and the German Cyber Defense: An Analysis of CERTs on Federal and State Level	191
13.1	Introduction	191
13.2	Related Work	193
13.3	Methodology: Empirical Study with German CERTs	198
13.4	Results	203
13.5	Discussion and Conclusion	214
14	Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey	221
14.1	Introduction	221
14.2	Related Work	223
14.3	Research Design	231
14.4	Results	234
14.5	Discussion	241
14.6	Conclusion	247

15	CySecAlert: An Alert Generation System for Cyber Security	
	Events Using Open Source Intelligence Data	249
15.1	Introduction	249
15.2	Concept	250
15.3	Evaluation	255
15.4	Related Work and Discussion	261
15.5	Conclusion	265
	Bibliography	267